驗證零信任安全白皮書

目錄

簡介

本文檔介紹與零信任相關的資訊，以及如何使用零信任保護企業。

執行摘要

零信任表示假設使用者、裝置或應用程式（無論是在網路外部還是在網路內部）都不能視為安全，並且必須驗證每個使用者或應用程式才能允許其訪問網路資產。

在虛擬化和將內部資源快速遷移到公共、私有和混合雲中，這一概念已變得更加重要。

「零信任」一詞由Forrester在2010年發佈其「零信任網路架構報告」時建立。

必須瞭解，零信任必須作為業務級別的策略來啟動，以保護重要的業務利益和計畫。

零信任支柱

什麼是零信任？

零信任是一種戰略方法，它包含各種技術，幫助為當今的基礎設施實現更切實的安全性。它是一個安全架構和企業方法，旨在有效地協調當今的技術、實踐和策略的組合。

它代表了我們在安全方法上的發展，提供了一種全面、可互操作的整體解決方案方法，該方法融合了多個供應商的產品和服務。

零信任基於許多已建立的技術，例如網路分段、多因素身份驗證和網路訪問控制。

零信任為何重要

零信任有助於保護企業免受未授權使用者、漏洞和網路攻擊。您可以持續驗證使用者和裝置的身份，僅允許他們執行其工作所需的許可權，從而最大限度地降低發生安全事件的風險。

市場研究表明，預計全球零託管證券市場規模將從2022年的估計值270億美元增至2027/2028年的約600億美元，當時的複合年增長率約為17%。

動機：

- 基於目標的網路攻擊頻率提高。
- 資料保護和資訊保安法規的不斷增長。
- 更需要降低業務和組織風險。
- 隨著越來越多的服務遷移到雲，集中化的資料部署超越了資料邊界，並放大了安全風險。
- 在整個訪問過程中確認使用者身份的需要，而不僅僅是最初的需要。

一次勒索軟體攻擊要花費500萬美元。網路犯罪分子在對待企業時不會有所歧視。

最近的CIO和CISO調查顯示，零信任是五大優先事項之一。CISO表示，向遠端工作的轉變、勞動力短缺以及網路安全攻擊的大幅增加要求他們企業中的現有系統受到保護。

傳統與零信任模型

傳統環境是在環境構建之後新增安全性的環境。通常情況下，它們是平面網路，其防禦是圍繞網路邊緣構建的，用於防止來自Internet的攻擊。

零信任通常被認為專注於通過加密、安全的電腦協定、動態工作負載以及資料級別的驗證和授權相結合的方式在多個級別保護組織的系統和資料的需要，而不只依賴外部網路邊界。

傳統以外圍環境為中心的安全架構效率較低，因為工作負載越來越多地從雲交付，而移動終端已成為應用和資料存取的規範。

零信任架構框架

零信任架構框架處理對系統、應用和資料資源的訪問限制，這些限制適用於那些特別需要訪問並已經過驗證的使用者和裝置。它們必須持續進行身份認證和安全狀態認證，以確保每個資源獲得適當的授權以提供訪問許可權。

該框架基於NIST特別出版物800-207，旨在提供將零信任安全概念遷移並部署到企業環境的路線圖。

有效的零信任架構框架可協調並整合這七個主要核心元件。

- 零信任網路是零信任策略的一個重要特徵，是指對網路進行分段或隔離網路資產，以及保持對網路之間通訊的控制。此外，它還保護可信連線，以擴展工作空間以供遠端使用。
- 零信任員工隊伍包含限制和強制使用者訪問的方法，其中包括對使用者進行身份驗證以及持續監控和管理其訪問許可權的技術。此存取由DNS、多重驗證和網路加密等技術加以保護。
- 零信任裝置解決了隔離、保護和管理所有聯網裝置的需要，這些裝置隨著移動性和物聯網的增加而增長，為攻擊者製造了極大的漏洞。
- 零信任工作負載可保護運行關鍵業務流程的前後應用堆疊。重點保護資料中心中應用、資料和服務之間的東/西流量，以更好地保護關鍵應用。
- 零信任資料是指對資料進行分類和分類的方法，並結合技術解決方案來保護和管理資料（包括資料加密）。
- 可視性和分析是指為自動化和協調提供感知，使管理員不僅能夠看到而且能夠瞭解其環境中的活動（包括即時威脅的存在）的技術。
- 自動化和協調包括機器學習演算法和人工智慧等工具和技術，用於自動對網路和資料中心資產進行分類，並建議和應用自動實施的分割和安全措施、策略和規則；因此，可減輕安全團隊的負擔並加速攻擊緩解。

零信任和分段

每個基於網路的資源都必須以最小特權的原則進行保護和分段。這最好通過資產管理系統來實現

，該系統可以控制各種用途的憑證和訪問許可權。

零信任分段需要包括品牌保護、有限的攻擊面、提高的網路穩定性以及支援快速服務部署。

為了進一步實現對單個資源的保護，可以使用微分段。在乙太網幀中插入標籤值以唯一地標識資源的情況下，可以使用可擴展組標籤(SGT)。此外，基礎設施裝置包括智慧交換機、路由器或下一代防火牆，這些裝置可用作網關裝置來保護每項資源。

可視性、分析和自動化

必須全面瞭解組織的所有資產以及與這些資產關聯的任何活動。這是零信任的基礎。

為了提供動態的政策和信任決策，需要不斷收集分析。我們的零信任架構方法側重於SDN策略的核心邏輯元件，使用策略引擎和策略管理員形成一個控制平面，以限制通過資料平面中的策略實施點訪問資源。

零信任架構提供更好的網路環境、學習和保證，以安全地完成任務所需的功能：

- 對使用者、裝置、應用、工作負載和資料的訪問進行細粒度細分。
- 執行安全策略的任意位置，包括LAN、WAN、資料中心、雲和邊緣。
- 全面的身份管理 — 將身份和訪問管理擴展到包括使用者、裝置、應用、工作負載和資料的身份，這些身份通過軟體定義的訪問成為新的微型邊界。
- 利用全球威脅情報和源的整合威脅防禦。
- 對組織網路進行完全自動化、靈活的控制，以按照實現目標所需的規模、效能和可靠性安全運行。

零信任步驟

全面零信任安全的關鍵是將安全擴展到整個網路環境，無論是LAN、資料中心、雲邊緣還是雲。合規性當然是強制性的。

此安全必須包括您組織的網路環境的全面可視性。全面零信任中心的關鍵步驟如下：

- 識別裝置和敏感資料。執行裝置、敏感資料和工作負載的識別和分類。
- 瞭解您的敏感資料流。
- 設計您的零信任分段策略。每個基於網路的資產都必須以最小許可權原則進行保護和適當分段，並嚴格實施精細控制，以便使用者僅能訪問執行任務所需的資源。
- 實施策略和狀態。這可以通過Cisco DNAC或ISE等平台執行。
- 持續監控零信任環境。實施安全分析以即時監控和分析安全事件並快速識別惡意活動。持續檢查並記錄內部和外部的所有流量。

實現可信訪問

要實現全面的零信任安全性，組織必須將其零信任方法擴展到整個員工、工作場所和工作負載。

- 零信任員工團隊 — 使用者和裝置必須經過身份驗證和授權，並且持續監控和管理訪問和許可權以保護資源。

- 零信任工作場所 — 必須控制整個工作場所（包括雲和邊緣）的訪問。
- 零信任工作負載 — 必須在整個應用堆疊(包括在雲中的容器、虛擬機器管理程式和微服務之間以及傳統機構資料中心之間實施精細訪問控制。

思科是Forrester認可的零信任領導者，是整個網路（現場和雲中）零信任實施的堅定倡導者。您不僅可以將您的思科網路基礎設施作為零信任架構的重要基礎，而且還可以瞭解其他有助於您的組織進行零信任旅程的關鍵思科零信任安全功能。

思科安全產品組合

可以使用以下內容構建成功的零信任框架：

- 通過Cisco Duo對使用者、裝置和應用進行無障礙、安全訪問
- 通過Cisco Umbrella實現靈活的雲安全
- 通過思科安全防火牆的智慧資料包檢測
- 通過安全終端(前身為AMP)進行高級惡意軟體防護
- 通過Cisco AnyConnect進行安全VPN和遠端訪問
- 通過Cisco Secure Analytics(前身為Stealthwatch)實現整體工作負載保護
- 使用思科身份服務引擎(ISE)保護的網路分段
- 通過思科安全工作負載實現應用可視性和微分段
- 通過Cisco SecureX的整合安全平台
- 統一的SASE解決方案，通過思科安全連線提供即服務訂用
- Cisco Zero Trust Strategy Service提供的專家指導
- 通過諮詢、諮詢和解決方案服務提供支援和端到端服務

摘要

零信任的一個最簡單的方法是「從不信任並始終驗證」。 這適用於每個網路連線、每個會話，以及訪問關鍵應用、工作負載和資料的每個請求。

零信任安全框架圍繞組織網路中的每個資源建立本地化的微邊界防禦。如果設計正確，這些框架可以保護資產，無論資產位於何處。

降低風險的有效方法是控制對特權及共用資料的訪問，並採用最小特權原則。此安全模型支援通過API進行協調，以及整合工作流自動化平台，從而提供對使用者和應用的可視性。

成功實施零信任有助於確保組織整個資訊科技環境的安全和無縫操作，並持續可靠地訪問組織的關鍵工作負載、應用程式和資料，從而增強組織的任務。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。